ON SECURITY AND PERFORMANCE ENHANCEMENT IN WIRELESS MESH NETWORKS

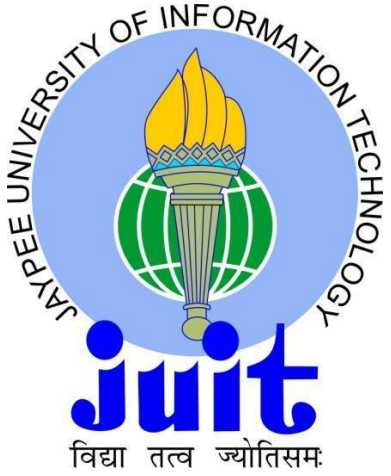
Synopsis submitted in fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

BY

GEETANJALI

Enrollment No. 146201



Under the supervision of

Dr. Hemraj Saini

Department of Computer Science and Engineering

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

Waknaghat, Solan-173234, Himachal Pradesh, INDIA

April, 2017

ABSTRACT

Wireless Mesh Network (WMN) is considered as a next generation key promising technology which is attractive in the areas where infrastructure is either existing or absurdly expensive because of multi-hop, self-healing, self-organizing and dynamic features. Advancement in networking technologies has allowed for organizations to use the network not only to share the resources but also to store large pool of data for analysis. Therefore, securing such data and resources of organization on a network is a big concern. Client, infrastructure and hybrid are the different types of WMN architectures consisting of two sorts of nodes; mesh routers (MR's) and mesh clients (MC's). MR's acts as backbone which provides the network services to the clients and responsible for forwarding the data packets to their intended destination nodes and MC's are the end point those accesses the network services via mesh routers. Whenever, a MC moves outside the boundary range of its current serving mesh router then the corresponding signal-to-noise ratio (SNR) of that serving MR will falls due to signal attenuation. A significant drop in SNR ratio makes the MC to search for a new mesh router having good signal strength for continuing its network services by triggering the handoff procedure. Since, the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network attacks and delay in the network. Therefore, during the handoff procedure, it is prerequisite that roaming clients ample access authentication process not only with a short delay but also with the fortification for the roaming clients with handoff networks. Further, if a node either inter-domain (communicate between two domains) or intra-domain (communicate within a domain) wants to send some messages to its intended destination node, the information is being passed among multiple MR's. However, to prevent the data exposure at each intermediate node, the messages must be encrypted by some security techniques or an ornate encryption technique which is required to guarantee that even if the message is forged by an intruder then it may not be able to decrypt it anyway. Due to the dynamic nature of WMN, where information is being passed over multiple hops or MR's, data encryption time is taken to be an important parameter. Furthermore, the most significant factor that impacts the WMN performance is the nature of fundamental routing protocols used for promoting the data packets. Presence of any malicious or misbehaving node within a routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network.

Although, numbers of scientists/researchers have proposed various handoff authentication procedures with message encryption and secure routing techniques, However, the issues arises by the intruders that encounters number of malicious nodes or threats to disrupt the network performance. In addition, by increasing one parameter such as to ensure the security, others parameters (such as end-to-end delay, network throughput, packet delivery ratio) get affected drastically. Therefore, there is a need to propose an efficient security technique having reduced authentication delay, less encryption/decryption time and secure routing mechanism against routing layer attacks with the aim of optimizing the other network parameters. Therefore, in order to provide an efficient and secure communication process, the security is ensured at three different aspects i.e. authentication of handoff clients, encrypted message transmission between source and destination and secure route discovery to route the transmitted data packets.

Table of Contents

	PAGE NO.
ABSTRACT	i-ii
1. INTRODUCTION	1-3
1.1 Motivation and Contribution	1-3
1.2 Organization of thesis	3-3
2. OBJECTIVES	3-12
2.1 Secure handoff process against wireless threats	4-7
2.1.1 Approach 1: Security in handoff process against malicious threats	4-6
2.1.2 Approach 2: Security in handoff process against malicious threats along with reduced authentication delay	6-7
2.2 Secure message transmission with reduced encryption/decryption time	7-9
2.3 Secure routing technique against wireless routing attacks	9-10
2.4 Application based scenario	10-12
2.4.1 Implementation of secure routing in smart home environments	11-11
2.4.2 Implementation of secure handoff routing process in smart home environments	11-12
3. CONCLUSION AND FUTURE WORK	12-12
4. REFERENCES	12-16
5. LIST OF PUBLICATIONS	17-19

1. INTRODUCTION

Wireless Mesh Network (WMN) is considered as a next generation key promising technology which is attractive in the areas where infrastructure is either existing or absurdly expensive because of multi-hop, self-healing, self-organizing and dynamic features [1, 2]. The multi-hop characteristic of WMN extends the scalability of the network where the number of nodes communicate in a multi-hop manner by acting as a host or a router to access or forward their intended data packets. Advancement in networking technologies has allowed for organizations to use the network not only to share the resources but also to store large pool of data for analysis. Therefore, securing such data and resources of organizations on a network is a big concern. The existing communication protocols are vulnerable to a variety of security threats i.e. worm hole attacks, black hole attacks, authentication delay, packet drop ratio and end-to-end delay [3-6] because of an assumption of non-hostile environment where nodes are cooperative and non-malicious. However, to prevent from these loop holes, an efficient and communication secure protocol is needed which can successfully transmit the data packets to their intended destination nodes [7-9]. Although researchers/scientists have proposed numerous security protocols, however, there exist number of security issues at different aspects of communication process and if one of the parameter is considered which is in order to ensure the security in the network, other parameters such as network delay, throughput and packet delivery ratio are affected drastically [10-15]. Therefore, there is a need to determine an efficient communication mechanism which can ensure the security along with improved network metrics.

1.1 MOTIVATION AND CONTRIBUTION

WMN consists of two sorts of nodes, mesh routers (MRs) and mesh clients (MCs). MRs provide the internet connectivity to MCs by forming a wireless backbone and are generally static or have minimal mobility in the network while MCs are mobile and access the network services via mesh routers [16-18]. Whenever, a MC moves outside the boundary range of its current serving mesh router, the signal-to-noise ratio (SNR) falls due to signal attenuation, therefore, the significant drop of SNR ratio makes the MC to search a new mesh router having good signal strength for improved network services by triggering the handoff in the network [19-24]. Since, the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network layer

attacks and delay. Further, during handoff procedure, it is prerequisite that roaming clients ample access authentication not only with a short delay but also with the fortification for the roaming clients as well as the handoff procedures. Therefore, the first research objective focuses on securing the handoff procedure against wireless security threats. Further, if a node either inter-domain (communication between two domains) or intra-domain (communication within a domain) wants to send some messages to their intended destination nodes; the transmitted information is passed through multiple hops or multiple MRs [25-29]. In order to prevent the data exposure at each intermediate node, the message must be encrypted by an ornate encryption technique which is requisite to guarantee that even if the message is forged it may not be able to decrypt it anyway. Whenever a MC (source node) wants to send some message to another MC (destination node), in order to protect its data from the intruders during the transmission process, the source node will encrypt its original message known as plain text into some encoded form known as cipher text by applying encryption algorithms. Although, there exist a number of techniques to encrypt the plain text message, however, a significant delay in encrypting or decrypting the message may invite a number of security threats that can cause reduced throughput with an increase in network delay. Therefore, there is a need to determine an encryption/decryption algorithm that takes less time and increases the network throughput during the message transmission process. Furthermore, the most significant factor that impacts the WMN performance is the nature of fundamental routing protocols used for promoting the data packets. Even though the client is authentic and messages are encrypted, presence of any malicious node within routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network [30-34]. Therefore, there is a need to propose a secure phenomenon at each level of network communication and establish a technique which is transparent to other routing mechanisms with improved network metrics. Therefore, the contribution with respect to secure communication mechanism is briefed in the following steps:

- Ensuring the client authenticity during the handoff procedure.
- An efficient encryption/decryption technique that ensures the message security with less delay provides high throughput by avoiding the attacking strategies.
- A secure routing mechanism needed to route the data traffic between their intended source and the destination.

- An application based scenario such as smart home application that validates and verifies the previously proposed mechanisms to ensure the security and performance at different aspects.

1.2 ORGANIZATION OF THE THESIS

The organization of thesis is divided into seven chapters as given below. The introduction, research background, problem statement, research scope and research objectives are reported in CHAPTER 1. In this chapter the need of security in current wireless technology which is WMN is discussed. Further, the research subareas with their problem statements are covered in this chapter. CHAPTER 2 evidences the background and preliminaries for the research in this thesis. This chapter states the architecture of WMN with its benefits, applications and authentication protocols is briefed. Further, the security issues that arise at each level of WMN are also elaborated in this chapter. CHAPTER 3 deals with the need of security during handoffs in WMN. The secure handoff approach is proved by showing the simulation results. CHAPTER 4 presents the data encryption approach during transmission between source and destination. CHAPTER 5 presents the generic approach for secure routing in WMN. This chapter briefs the results for the proposed approach with proper simulation results. CHAPTER 6 validates the above mentioned three problems of chapter 3, 4 and 5 through an application based scenario such as smart home application. The results are verified by showing a rigorous comparative study between proposed approaches and existing approaches in terms of certain network metrics. Further, CHAPTER 7 concludes the thesis that includes the thesis summary, concluding remarks, contribution of the work done and suggestions for the future scope in this field.

2. OBJECTIVES

In order to provide a secure communication process, there is a need to ensure an efficient authentication process, message transmission and routing mechanism between the communicating entities. Therefore, the first objective is to authenticate the handoff mesh clients which are able to securely transmit their messages by choosing a secure routed path to their intended destination nodes in order to ensure an efficient and secure communication mechanism, the security is described at three aspects of communication process 1) handoff authentication of mesh clients, 2) secure message transmission and 3) trust among the routing nodes.

2.1 SECURE HANDOFF PROCEDURE AGAINST WIRELESS THREATS

Research communities have designed several handoff routing protocols for WMN, however, there is a need to improve the performance metrics based on security and resilient nature of handoff routing protocols. The multi-hop, ticket based and proactive key distributions are some recent authentication techniques to ensure the security during mobility in mesh environments. Nevertheless, a significant delay to compute and verify the security process and authenticity of legitimate user may enforce to introduce number of internal vulnerabilities [35-39] to come. In this, we have proposed two handoff security techniques over an existing handoff approach.

2.1.1 HANDOFF SECURITY AGAINST MALICIOUS THREATS

Although the author [37] has proposed a ticket based technique for handoff by defining the procedure in two different phases, i) ticket issuing phase which is used to generate the tickets for handoff procedure while ii) re-authentication phase which is done in the actual handoff authentication. In this approach, each mesh router and mesh client stores the keys and the tickets of their domains into their databases. During handoff procedure, whenever, a MC enters into the foreign mesh router's domain to access the services, MRs communicates with each other to know the domain and to get the ticket and the key of the servicing MC to authenticate its legitimacy. In this approach communication between MRs may indulge a number of security threats i.e. DoS attack, message forging attacks and lead to significant delay and communication overhead which is a limitation. Further, the storage of keys and tickets at MCs involves several resource constraints such as memory, energy consumption and storage problems. Moreover, attackers can easily attack on MCs and communicating MRs to forge or modify the data and affect the network performance by adding the delay in process. In a summary none of the existing techniques provide guarantee for reduced authentication delay [40-43] and resilient against security attacks [44-47]. So, the main focus of the proposed protocol is to reduce authentication delay, request delay and ensure a secure communication under various security threats. The proposed scheme is analyzed against ticket based handoff technique [48] where the objective of handoff protocol is to support an efficient handoff process in a secure manner. The major difference between proposed protocol and existing ticket based handoff is that in our scheme, keys and tickets are generated and stored by AS while in ticket based handoff, tickets and keys are generated by AS but stored at MRs and MCs which may lead to resource constraint problems i.e. storage overhead

and vulnerabilities towards several security threats. Further, our scheme is resistant against user privacy, black hole, forgery and denial of service attacks as there is no direct link of AS with the mesh clients or an attacker. The technical contribution of the paper is described as follows, 1) Ticket generating-assigning phase that is used to generate the keys and the tickets between communicating nodes and 2) Handoff authentication phase which explains the actual handoff procedure in the network. The flowchart of the corresponding proposed mechanism is depicted in Figure 1.

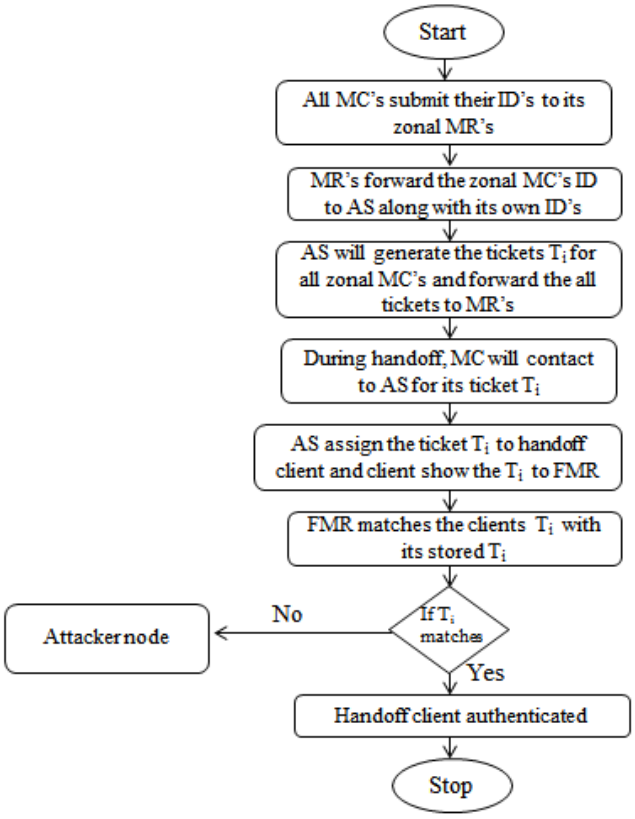

Start
All MC's submit their ID's to its zonal MR's
MR's forward the zonal MC's ID to AS along with its own ID's
AS will generate the tickets T_i for all zonal MC's and forward the all tickets to MR's
During handoff, MC will contact to AS for its ticket T_i
AS assign the ticket T_i to handoff client and client show the T_i to FMR
FMR matches the clients T_i with its stored T_i
If T_i matches
No
Attacker node
Yes
Handoff client authenticated
Stop

Figure 1 Flowchart of the proposed handoff mechanism

The proposed approach is both centralized in case of handoff and distributed during normal communication which may reduce the extra overhead of key management at server side. The technique is simulated and analyzed over NS2 simulator under different probabilistic scenarios of authentication delay, request delay and is legitimated by discussing an empirical study over certain security threats against reported literature. The depicted figure 2 shows the graphs of proposed mechanism in comparison of existing approach.

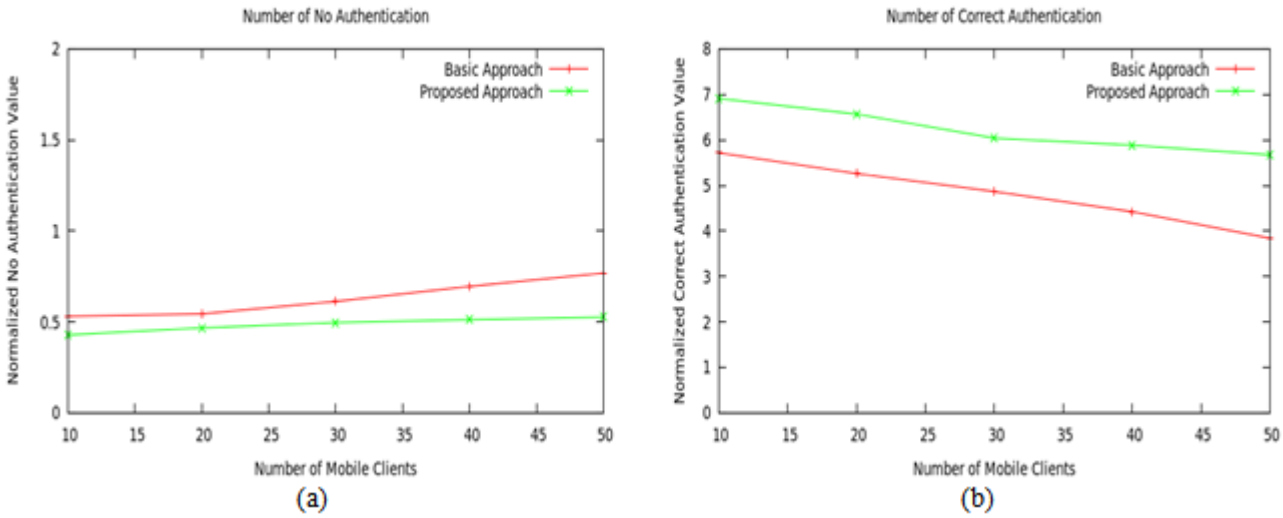


Figure 2 comparisons of both approaches against (a) no authentication value and (b) correct authentication value

2.1.2 HANDOFF SECURITY AGAINST MALICIOUS THREATS ALONG WITH REDUCED AUTHENTICATION DELAY

However, the problem that exists with the previously proposed approach is authentication delay.

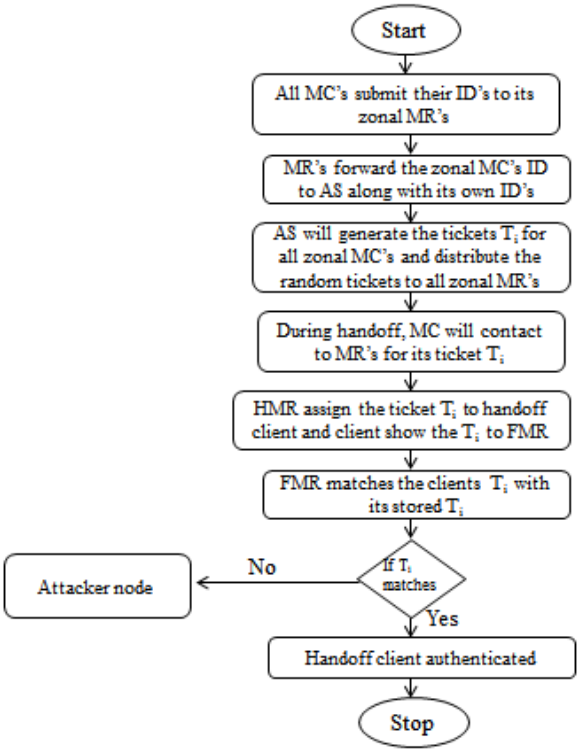

Start
All MC's submit their ID's to its zonal MR's
MR's forward the zonal MC's ID to AS along with its own ID's
AS will generate the tickets T_i for all zonal MC's and distribute the random tickets to all zonal MR's
During handoff, MC will contact to MR's for its ticket T_i
HMR assign the ticket T_i to handoff client and client show the T_i to FMR
FMR matches the clients T_i with its stored T_i
If T_i matches
No
Attacker node
Yes
Handoff client authenticated
Stop

Figure 3 Flowchart of the extended secure handoff mechanism

As the mesh clients need to communicate with the authentication server through various mesh routers to access their tickets this may increase the authentication delay between the server and mesh clients. Therefore, to overcome this issue, the proposed approach is modified where instead of communicating with the authentication server, the mesh clients will directly communicate with the mesh router. The authentication server will distribute the tickets to their intended domains mesh routers where instead of storing the entire tickets, the routers will store some random tickets distributed by the authentication server. The figure 3 depicts the extended proposed mechanism of ticket generation and distribution. The proposed approach is distributed during communication which may reduce the extra overhead of key management at server side. The technique is simulated and analyzed over NS2 simulator under different probabilistic scenarios of authentication delay, request delay as depicted in figure 4 and is legitimated by discussing an empirical study over certain security threats against reported literature.

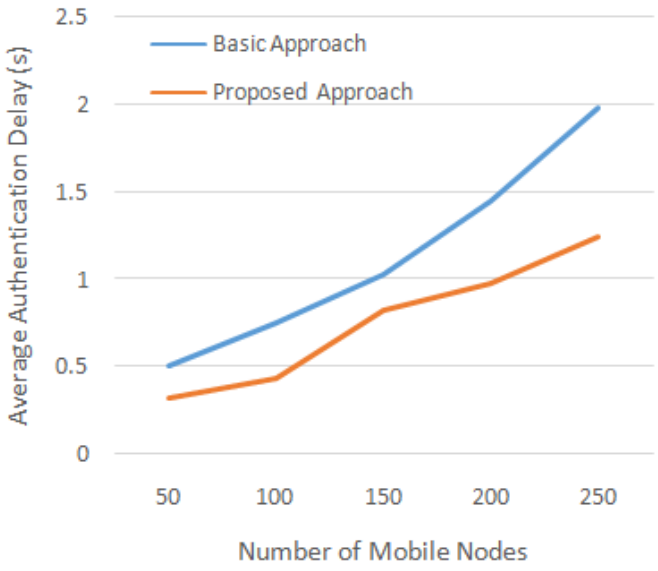


Figure 4 Reduced authentication delay

2.2 SECURE MESSAGE TRANSMISSION WITH REDUCED ENCRYPTION/DECRYPTION TIME

Due to the nature of WMN where information is being passed over multiple hops, data encryption is taken to be an important parameter. Wireless Mesh Network (WMN) is deliberated as a key technology due to its self-healing and self-configuring characteristics with the provisions of large scale exposure in industrial and academic fields.

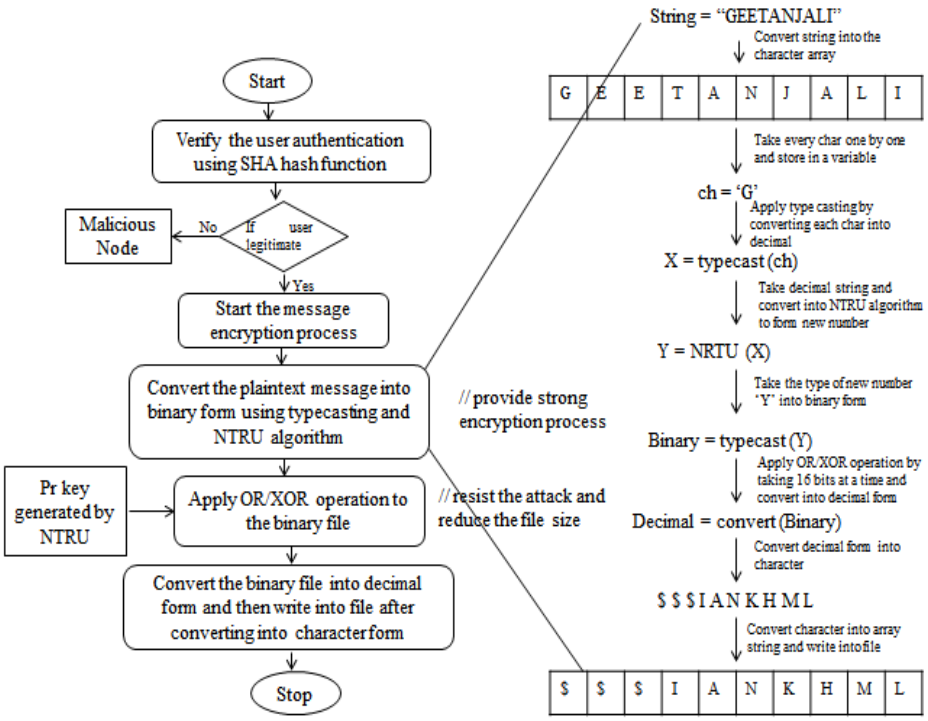

Start
Verify the user authentication using SHA hash function
Malicious Node
No
If user legitimate
Yes
Start the message encryption process
Convert the plaintext message into binary form using typecasting and NTRU algorithm
// provide strong encryption process
Pr key generated by NTRU
Apply OR/XOR operation to the binary file
// resist the attack and reduce the file size
Convert the binary file into decimal form and then write into file after converting into character form
Stop
String = "GEETANJALI"
Convert string into the character array
G E E T A N J A L I
Take every char one by one and store in a variable
ch = 'G'
Apply type casting by converting each char into decimal
X = typecast (ch)
Take decimal string and convert into NTRU algorithm to form new number
Y = NRTU (X)
Take the type of new number 'Y' into binary form
Binary = typecast (Y)
Apply OR/XOR operation by taking 16 bits at a time and convert into decimal form
Decimal = convert (Binary)
Convert decimal form into character
$ $ $ I A N K H M L
Convert character into array string and write into file
$ $ $ I A N K H M L

Figure 5 Flowchart of proposed message encryption algorithm

Security is considered as a vital constraint in WMN owing to its broadcasting and dynamic nature. Due to nature of WMN where information is being passed over multiple hops, data encryption is taken to be an important parameter. Although researchers have proposed various encryption techniques to provide the message security, however, foremost shortcoming in most of the approaches is their processing time. An encryption technique having large encryption/decryption timing increases overhead which may cause copious perilous attacks (i.e. passive eavesdropping etc.). Further an encryption technique with large file size may increase the load on the server during file transmission [49-53]. In order to overcome these hitches, the manuscript proposes an end to end encryption based on algebraic operations i.e. Advanced Encryption through Homomorphic operation (AEHO) with reduced processing time where a cipher text is generated using OR/XOR operations. Further, a Trusted Party Authority (TPA) server is anticipated to provide the authenticity. Figure 5 depicts the flowchart of proposed encryption mechanism. To establish the legitimacy of the proposed solution, the experimental results are explained in terms of reduced encryption/decryption timing and increased throughput as depicted in figure 6.

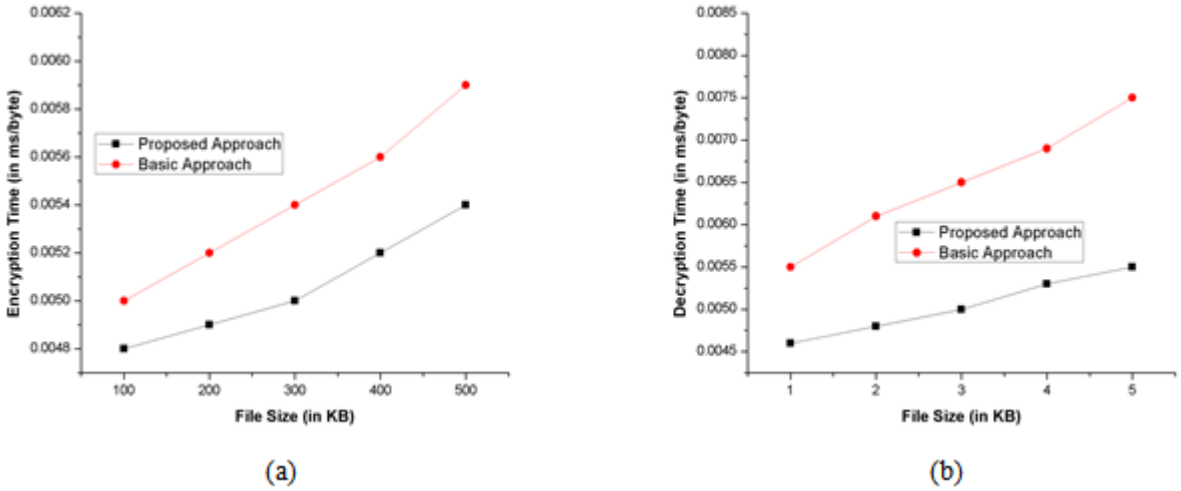


Figure 6 Comparisons between proposed and basic approach (a) encryption time (b) decryption time

2.3 SECURE ROUTING TECHNIQUE AGAINST WIRELESS ROUTING ATTACKS

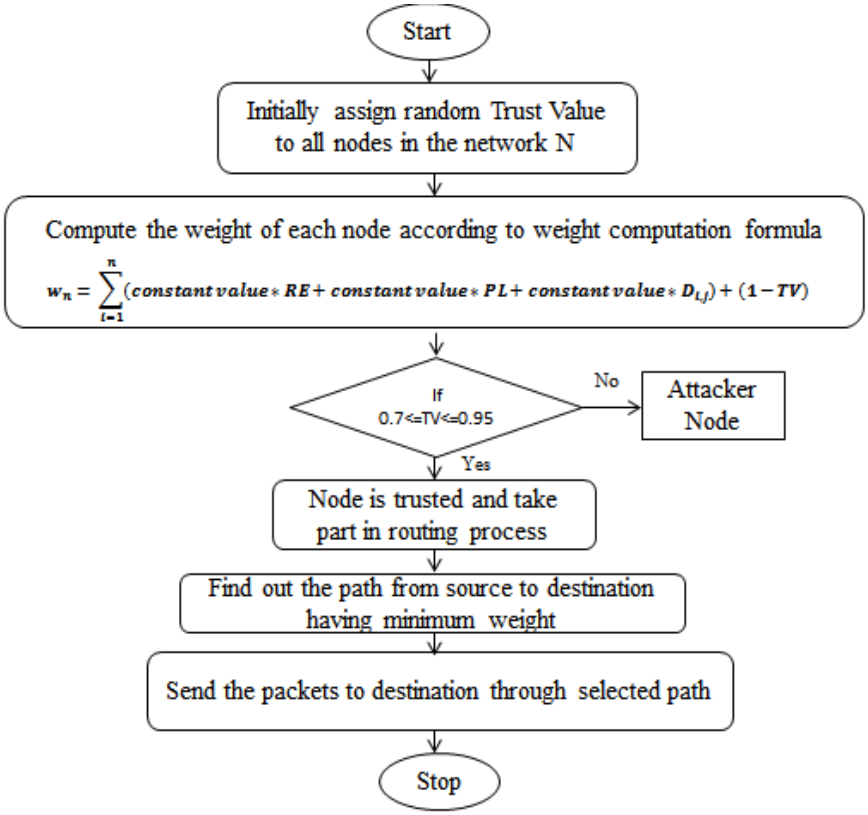

Start
Initially assign random Trust Value to all nodes in the network N
Compute the weight of each node according to weight computation formula
$w_n = \sum_{i=1}^{n} (constant\ value * RE + constant\ value * PL + constant\ value * D_{i,j}) + (1 - TV)$
If 0.7<=TV<=0.95
No
Attacker Node
Yes
Node is trusted and take part in routing process
Find out the path from source to destination having minimum weight
Send the packets to destination through selected path
Stop

Figure 7 Flowchart of proposed secure routing mechanism

In this chapter, dijkstra's shortest path routing algorithm is used where weights are deliberated using certain parameters (i.e. node distance, node's previous interactions, packet loss percentage and trust values of each node) for providing the security against routing attacks [54-56]. The malicious nodes involved during route discovery process are eliminated by calculating the trust of each node using Social Impact Theory Optimizer (SITO). Here, we have discussed the network performance trade-off caused by secure path formation in conventional methods and proposed a Weight Trusted Routing (WTR) mechanism for eliminating these issues (packet-loss ratio, end-to-end delay and route discovery delay). We have numerically simulated and compared the network metrics for both conventional and proposed approaches. Moreover, the proposed technique is validated (through an adversary model) by discussing an empirical study over routing attacks. The flow chart of proposed mechanism is presented by figure 7. The proposed WTR mechanism enhances the network metrics by reducing additional cryptographic operations to ensure the security. Further, the proposed protocol is analyzed against reported routing protocol i.e. Secure Routing Mechanism (SRM) which overcomes the routing attacks (i.e. black hole and worm hole attacks) by modifying the basic AODV protocol as depicted in figure 8.

2.4 APPLICATION BASED SCENARIO

This chapter exploits the proposed security mechanisms over an application based scenario. With the recent societal development, the demand of digital environments where the humans interact smartly with their surroundings to increase their comfort zone as compared to the hard build infrastructures which is a challenging task.

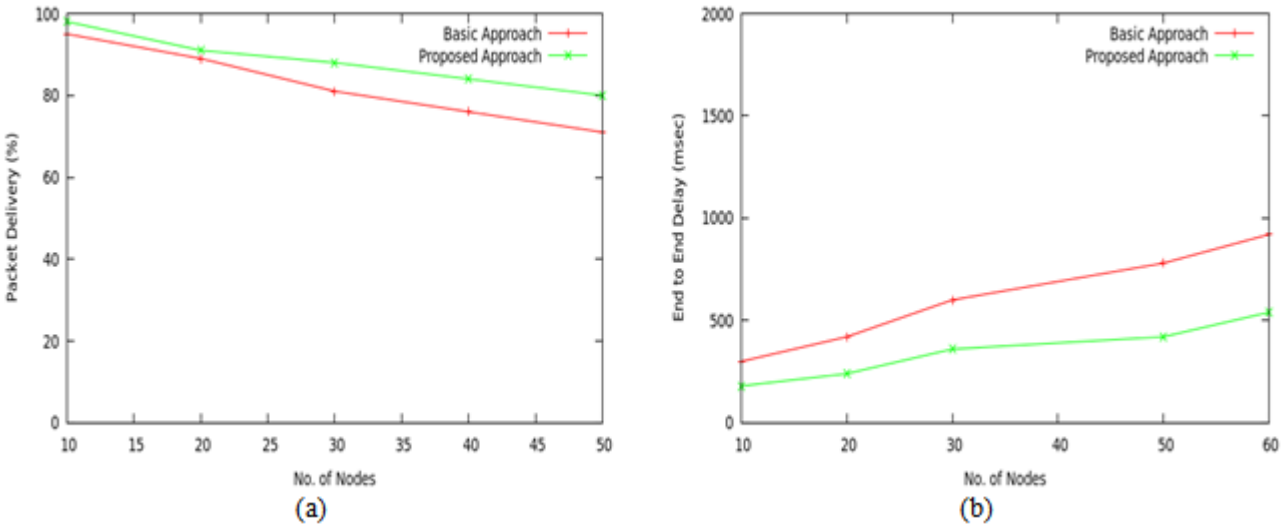


Figure 8 comparison metrics (a) packet delivery ratio and (b) end-to-end delay

To enhance the coverage area by introducing additional placements of devices and to manage the continuous changes of concerned systems, there is a need to use a more efficient, robust and reliable communication standard such as Zigbee, Bluetooth or Wi-Fi to provide the interconnectivity among the devices. Currently, Zigbee is one of the most widely used wireless technology for such systems due to its mesh based architecture which allows high scalability and large coverage area by incorporating self-healing, self-organizing and self-configuring characteristics. In this chapter, we have exploited the routing and handoff process over smart home application.

2.4.1 SECURE ROUTING IMPLEMENTATION IN SMART HOME ENVIRONMENTS

In order to ensure secure routing mechanism, weight trusted routing (WTR) mechanism is used to detect and eliminate the malicious nodes involved during the routing path formation for the smart home environments where the routing between communicating entities is performed through mesh architecture. However, to ensure the security against malicious behavior of nodes, the proposed mechanism uses dijkstra's shortest path routing algorithm in which the weights are deliberated using certain parameters such as node distance, node's previous interactions, packet-loss percentage and trust values of each node. The malicious nodes involved during route discovery process are eliminated by computing the trust of each node using Social Impact Theory Optimizer (SITO). In addition to this, we have discussed the network performance trade-off caused by the secure path formation with conventional method and have proposed a WTR mechanism for eliminating potential issues such as packet-loss ratio, end-to-end delay and throughput. Further, routing and handoff procedures are simulated in smart home environments to analyze the combined results of network metrics. NS2 version 2.35 simulator is used to simulate and compare the network metrics for both conventional and proposed approaches over smart home environments and is validated through experimental results over end-to-end delay and message delivery ratio against reported literature.

2.4.2 SECURE HANDOFF ROUTING IMPLEMENTATION IN SMART HOME ENVIRONMENTS

The secure routing mechanism is extended over handoff procedures where mesh clients or devices are mobile in nature. During the mobility, the security is checked after authenticating the mesh clients or devices and securely route their data transmission against number of routing

layer threats. Black hole and data falsification attacks are considered to analyze the proposed mechanism because of their severe malicious characteristics. The proposed mechanism is simulated and analyzed over NS2 simulator against previously proposed handoff and routing mechanisms by measuring their certain network metrics such as throughput, end-to-end delay, and packet drop ratio against black hole and data falsification attacks.

3. CONCLUSION AND FUTURE WORK

In order to provide a secure communication mechanism, the security is ensured at three different aspects of communication process. A trusted third party handoff authentication technique is proposed that ensures the clients legitimacy during the mobility and provides the significant results against authentication delay, probabilistic authentication scenarios and mobility delay. Further, to secure the transmitted message between source and destination, a secure homomorphic technique is proposed that significantly reduces the encryption/decryption time along with better results against processing delay and attacking strategies. Moreover, a secure routing procedure is provided to ensure the security from intermediate nodes involved during message transmission. The proposed routing technique is analyzed against certain networking parameters along with different routing layer attacks that significantly show better results as compared to traditional approaches. Furthermore, a smart home application scenario is considered to measure the proposed secure routing mechanism against certain networking parameters and finally both proposed handoff and routing techniques are considered to analyze the combined results against defined networking model by highlighting the better results as compare to traditional handoff and routing approaches. However, the energy consumption in the large number of network sizes during the packet transmission/reception is a potential issue which will be reported in future communication.

REFERENCES

1. Akyildiz, I. F., & Wang, X. A survey on wireless mesh networks. *IEEE Communications Magazine*, vol. 43, no. 9, pp. 23-30, 2005.
2. Akyildiz, I.F., Lee, W.Y., Vuran, M.C. and Mohanty, S., "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey", *Computer networks*, vol. *50, no.* 13, pp.2127-2159, 2006.
3. S. Khan & A.S.K. Pathan, Wireless networks and security issues, challenges and research trends"", *Springer science & business Media*, London, 2013.

4. A.S.K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET, CRC press, *Auerbach publications, Taylor & francis group,* U.S.A, 2016.
5. M. Erdelj, E. Natalizio, K.R. Chowdhury & I.F. Akyildiz, "Help from the Sky: Leveraging UAVs for Disaster Management", *IEEE Pervasive Computing*, vol. 16, no. 1, pp. 24-32, 2017.
6. H. Yang, H., Luo, F., Ye, S., Lu & L. Zhang, L. "Security in mobile ad hoc networks: challenges and solutions", *IEEE wireless communications*, vol. *11, no.* 1, pp.38-47, 2004.
7. R.D. Pietro, S. Guarino, N.V. Verde & J. Domingo, "Security in wireless ad-hoc networks–a survey", *Computer Communications*, vol. *51*, pp.1-20, 2014.
8. C.W. Lee, Security in wireless mesh networks", *Wireless Network Security*, Springer Berlin Heidelberg, pp. 229-246, 2013.
9. A. Hassanzadeh, Z., Xu, R., Stoleru, G., Gu & M. Polychronakis, "PRIDE: A practical intrusion detection system for resource constrained wireless mesh networks". *Computers & Security*, vol. *62*, pp.114-132, 2016.
10. R. Regan & J.M.L. Manickam, "A Survey on Wireless Mesh Networks and its Security Issues", *International Journal of Security and Its Applications*, vol. *10, no.* 3, pp.405-418, 2016.
11. E. Stevens, Y., Lin & V.W. Wong, "An MDP-based vertical handoff decision algorithm for heterogeneous wireless networks",. *IEEE Transactions on Vehicular Technology*, vol. *57, no.* 2, pp.1243-1254, 2008.
12. M. Tao, H., Yuan, X., Hong & J. Zhang, "SmartHO: mobility pattern recognition assisted intelligent handoff in wireless overlay networks", *Soft Computing*, vol. *20, no.* 10, pp.4121-4130, 2016.
13. G. Athanasiou & L. Tassiulas, "Design and implementation of distributed load balancing and fast handoff for wireless mesh networks", *Transactions on Emerging Telecommunications Technologies*, vol. *26, no.* 4, pp.630-649, 2015.
14. Y.M. Lai, P.J., Cheng, C.C., Lee & C.Y. Ku, "A New Ticket-Based Authentication Mechanism for Fast Handover in Mesh Network", *PloS one*, vol. *11, no.* 5, p.e0155064, 2016.
15. P. Xiao, J., He & Y. Fu, Y., "An access authentication protocol for trusted handoff in wireless mesh networks", *Computer Standards & Interfaces*, vol. *36, no.* 3, pp.480-488, 2014.
16. F. Wang, Y., Xu, H., Zhang, Y., Zhang & L. Zhu,"2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET", *IEEE Transactions on Vehicular Technology*, vol. *65, no.* 2, pp.896-911, 2016.
17. C. Lyu, D. Gu, Y., Zeng & P. Mohapatra, "PBA: prediction-based authentication for vehicle-to-vehicle communications", *IEEE Transactions on Dependable and Secure Computing*, vol. *13, no.* 1, pp.71-83, 2016.
18. S. Jiang, X., Zhu & L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs", *IEEE Transactions on Intelligent Transportation Systems*, vol. *17, no.* 8, pp.2193-2204, 2016.

19. S. Ravichandran, "Secured identity based approach wih privacy preservation for wireless mesh networks", *International journal of communication and networking system*. vol. 1, no. 2, pp. 1-8, 2012.
20. Y. Li, X. Cui, L. Hu & Y. Shen., "Efficient security transmission protocol with identity-based encryption in wireless mesh networks", *IEEE International Conference on High Performance Computing and Simulation (HPCS),* pp. 679-685, 2010.
21. L. Edward, P. Joseph, K.L. green, L.E. Riblett & J.M. Wisemanl., "Encryption in mobile wireless mesh networks", *IEEE International Carnahan Conference on Security Technology (ICCST),* pp. 1-6, 2012.
22. L. Li, T. Gu, L. Chang, Z. Xu, Y. Liu & J. Qian, "A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram", *IEEE Access*, vol 5, pp.1137-1145, 2017.
23. C.W. Ten, G. Manimaran & C.C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling", *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. *40, no.* 4, pp.853-865, 2010.
24. J.J. Jang & S. Nepal, "A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, vol. *80, no.* 5, pp.973-993, 2014.
25. P. Papadimitratos & Z.J. Haas, "Secure message transmission in mobile ad hoc networks", *Ad Hoc Networks*, vol. *1, no.* 1, pp.193-209, 2003.
26. J. Yao, S. Feng, X. Zhou & Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying", *IEEE Transactions on Communications*, vol. 64, no. 2, pp.753-764, 2016.
27. M. S. Obaidat, I. Woungang, S. K. Dhurandher & V. Koo, "A cryptography-based protocol against packet dropping and message tampering attacks on mobile ad hoc networks", *Security and Communication Networks*, vol. 7, no. 2, pp.376-384, 2014.
28. I. Woungang, S. K. Dhurandher, M. S. Obaidat & R. D. Peddi. "A DSR-based routing protocol for mitigating black hole attacks on mobile ad hoc networks", *Journal of Security and Communication Networks*, Wiley, vol. 9, no. 5, pp. 420-428, 2016.
29. D. Johnson & G. Hancke, "Comparison of two routing metrics in OLSR on a grid based mesh network", *Ad Hoc Networks*, vol. *7, no.* 2, pp.374-387, 2009.
30. J. Yi, A., Adnane, S. David & B. Parrein, "Multipath optimized link state routing for mobile ad hoc networks", *Ad Hoc Networks*, vol. *9, no.* 1, pp.28-47, 2011.
31. M. Ikeda, "Analysis of mobile ad-hoc network routing protocols using shadowing propagation model", *International Journal of Space-Based and Situated Computing*, vol. *2, no.* 3, pp.139-148, 2012.
32. X. Duan & X. Wang, "Authentication handover and privacy protection in 5G het nets using software-defined networking", *IEEE communications magazine*, Vol. 53, no. 4, pp. 28-35, 2015.
33. Q. Jiang, J. Ma, X. Lu & Y. Tian, "An efficient two-factor user authentication scheme with unlink ability for wireless sensor networks", *Journal of peer-to-peer networking and applications*, Vol. 8, no. 6, pp. 1070-1081, 2015.

34. X. Zhang, L. Guangsong & H. Wenbao. "Ticket-Based Authentication for Fast Handover in Wireless Mesh Networks", *Wireless Personal Communications*, vol. 85, no.3, pp. 1509-1523, 2015.
35. P. Xiao, J., He & Y. Fu, "An access authentication protocol for trusted handoff in wireless mesh networks", *Computer Standards & Interfaces*, vol. *36, no.* 3, pp.480-488, 2014.
36. S. Sivagurunathan & K. Prathapchandran, "Trust-Based Security Mechanisms for Self-Organized Networks (SONs)", *Self-Organized Mobile Communication Technologies and Techniques for Network Optimization*, pp. 92-114, 2016.
37. L. Xu, Y. He, X. Chen, & X. Huang, "Ticket-based handoff authentication for wireless mesh networks", *Computer networks*, Vol. 73, pp. 185-194, 2014.
38. Yu, Y., Li, K., Zhou, W. & Li, P., "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", *Journal of network and computer applications*, vol. *35, no.* 3, pp.867-880, 2012.
39. A.A. Bhosle, T.P. Thosar & S. Mehatre, "Black-hole and wormhole attack in routing protocol AODV in MANET", *International Journal of Computer Science, Engineering and Applications*, vol. *2, no.* 1, pp.38-45, 2012.
40. A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik & D. Goeckel, "Energy-Efficient Routing in Wireless Networks in the Presence of Jammingl", *IEEE Transactions on Wireless Communications*, vol. *15, no.* 10, pp.6828-6842, 2016.
41. R. Poovendran & L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks", *Wireless Networks*, vol. *13, no.* 1, pp.27-59, 2007.
42. I. Khalil, S. Bagchi & N.B. Shroff, "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks", *Ad Hoc Networks*, vol. *6, no.* 3, pp.344-362, 2008.
43. F. Guo, Y. Mu, W. Susilo, H. Hsing, D. Wong & V. Varadharajan, "Optimized Identity-Based Encryption from Bilinear Pairing for Lightweight Devices", *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 211-220, 2015.
44. Y. Li, X. Cui, L. Hu & Y. Shen. "Efficient security transmission protocol with identity-based encryption in wireless mesh networks", *IEEE International Conference on High Performance Computing and Simulation (HPCS)*, pp. 679-685, 2010.
45. L. Edward, P. Joseph, K.L. green, L.E. Riblett & J.M. Wisemanl. "Encryption in mobile wireless mesh networks", *IEEE International Carnahan Conference on Security Technology (ICCST)*, pp. 1-6, 2012.
46. D.M. Van, C. Gentry, S. Halevi & V. Vaikuntanathan, "Fully homomorphic encryption over the integers", *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, pp. 24-43, 2010.
47. C. Gentry, H. Shai & P. S. Nigel. "Fully homomorphic encryption with polylog overhead." *Advances in Cryptology EUROCRYPT*, Springer Berlin Heidelberg, pp. 465-482, 2012.
48. L. Li, T. Gu, L. Chang, Z. Xu, Y. Liu & J. Qian, "A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram", *IEEE Access*, vol 5, pp.1137-1145, 2017.

49. M. Kaliappan & B. Paramasivan, "Enhancing secure routing in mobile ad hoc Networks using a Dynamic Bayesian Signalling Game model", *Computers & Electrical Engineering*, vol. 41, pp. 301-313, 2015.
50. S. Khan, N.A. Alrajeh & K.K. Loo. "Secure route selection in wireless mesh networks", *Computer Networks*. vol. 56, no.2, pp. 491-503, 2012.
51. J. Yao, S. Feng, X. Zhou & Y. Liu, Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying", *IEEE Transactions on Communications*, vol. 64, no. 2, pp.753-764, 2016.
52. M. Martin & L. Lhotska. *Social impact theory based optimizer Advances in Artificial Life*, Springer Berlin Heidelberg. pp. 635-644, 2007.
53. S.U. Rehman & S. Manickam, "A study of smart home environment and its security threats", *International Journal of Reliability, Quality and Safety Engineering*, vol. 23, no. 3, pp. 1-9, 2016.
54. A. Neumann, E. Lopez, L. Cerdà-Alabern & L. Navarro, "Securely-entrusted multi-topology routing for community networks", *Proceedings of 2016 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, Italy , pp. 1-8, 2016.
55. P. Kumar, A. Gurtov, J., Iinatti, M., Ylianttila & M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments", *IEEE Sensors Journal*, vol. 16, no. 1, pp. 254-264, 2016.
56. T.D. Mendes, R. Godina, E.M., Rodrigues, J.C., Matias, J.C. & J.P. Catalao, "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources", *Energies*, vol. 8, no. 7, pp. 7279-7311, 2015.

PUBLICATIONS LIST

Published Journal Papers

1. G. Rathee and H. Saini. "Secure modified ad-hoc on-demand distance vector (MAODV) routing protocol", *International Journal of Mobile Computing and Multimedia Communications*, vol. 8, no. 1, pp. 1-18, 2017

   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

2. G. Rathee and H. Saini. "A Secure Buffer based Routing Protocol (SBRP) for WMN", *International Journal of Business Data Communications and Networking (IJBDCN)*, vol. 13, no. 1, pp. 28-44, 2017.

   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

3. G. Rathee and H. Saini. "Secure Handoff Technique with Reduced Authentication Delay in Wireless Mesh Network", *International Journal of Advanced Intelligence Paradigms* (in press).

   [Major indexing: SCOPUS (Elsevier), DBLP, ACM Digital Library, Academic OneFile (Gale), Educational Research Abstracts]. Online link: http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijaip

4. G. Rathee and H. Saini. "End-to-End Encryption by Algebraic OR/XOR", *International Journal of Control Theory and Applications*, vol. 9, no. 10, pp. 4819-4831, 2016.

   [Major indexing: SCOPUS, EBSCOhost].

5. G. Rathee and H. Saini. "A Secure Multicast Routing Protocol against Gray Hole Attack", *APRN Journal of Engineering and Applied Sciences*, vol. 11, no. 21, pp. 1-8, 2016.

   [Major indexing: SCOPUS, DBLP, Google scholar].

6. G. Rathee and H. Saini. "Security Concerns with Open Research Issues of Present Computer Network", *International Journal of Computer Science and Information Security*, vol. 14, no. 4, pp.406-432, 2016.

   [Major indexing: ESCI, IP & Science, Thomson Reuter, Web of Science].

7. G. Rathee and H. Saini. "Efficient Handoff Routing (EHR) in WMN", *International Journal of Computer Applications*, vol. 1, pp. 29-34, August 2016.

   [Major indexing: Google scholar, Proquest, EBSCO.]

Accepted Journal Papers

8. G. Rathee and H. Saini. "Weight Trusted Routing Mechanism for Hierarchical Mesh Environments", *International Journal of Distributed Systems and Technologies (IJDST)*. vol. 8, no. 3, pp. xx-xx, 2017.

   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

9. G. Rathee and H. Saini. "Authentication through Elliptic Curve Cryptography (ECC) Technique in WMN", *International Journal of Information Security and Processing*, vol. xx, no. xx, pp. xx-xx, 20xx.

   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

Published Book Chapters

10. G. Rathee and H. Saini (2016), "Mitigation Techniques for Gray Hole and Black Hole Attacks in Wireless Mesh Network", Proceedings of the International Congress on Information and Communication Technology, Springer, Singapore, pp. 383-392.

    [Major indexing: SCOPUS, DBLP, Google scholar].

11. G. Rathee, H. Saini and S.P. Ghrera (2016), "Secured Authentication and Signature Routing Protocol for WMN (SASR)", Proceedings of the Second International Conference on Computer and Communication Technologies, Springer, USA, pp. 327-336.

[Major indexing: SCOPUS, DBLP, Google scholar].

12. G. Rathee and H. Saini (2016), "A Secure Homomorphic Routing Technique in Wireless Mesh Network (HRT for WMN)", Information Systems Design and Intelligent Applications, Springer, USA, pp. 437-444.

    [Major indexing: SCOPUS, DBLP, Google scholar].

Published Conference Proceedings

13. G. Rathee and H. Saini (2016), "A Fast Handoff Technique in Wireless Mesh Network (FHT for WMN)", *Procedia Computer Science*, vol. 79, pp.722-728.

    [Major indexing: SCOPUS, Conference Proceedings Citation Index].

14. G. Rathee and H. Saini (2015), "On Reduced Computational Cost, Efficient and Secure Routing (ESR) for Wireless Mesh Network", *Procedia Computer Science*, vol. 58, pp.333-34.

    [Major indexing: SCOPUS, Conference Proceedings Citation Index].

Communicated Journal Papers

15. G. Rathee and H. Saini. "Weight Trusted Routing Implementation in Smart Home Environments", *Wireless Personnel Communication*. (submitted second revision) February, 2017.

[Major indexing: SCIE, SCOPUS, SCI mago, Google scholar, ACM digital Library].

16. G. Rathee and H. Saini. "Reduced Handoff Authentication Technique in Wireless Mesh Network", *Frontier of Information Technology and Electronic Engineering* (communicated)

[Major indexing: SCIE, SCOPUS, SCI mago, Google scholar, ACM digital Library].

17. G. Rathee and H. Saini. "Implementation of Secure Handoff Routing in Smart Home Environments", *Wireless Networks* (communicated)

[Major indexing: SCIE, SCOPUS, SCI mago, Google scholar, ACM digital Library].

Candidate's Signature